(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 606 007 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
05.02.2020 Bulletin 2020/06

(21) Application number: **18772511.4**

(22) Date of filing: **19.03.2018**

(51) Int Cl.:
H04L 29/08 *(2006.01)*

(86) International application number:
PCT/CN2018/079460

(87) International publication number:
WO 2018/171550 (27.09.2018 Gazette 2018/39)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
KH MA MD TN

(30) Priority: **21.03.2017 CN 201710170866**

(71) Applicant: **Tencent Technology (Shenzhen) Company Limited**
Shenzhen, Guangdong 518057 (CN)

(72) Inventor: **XIAO, Xiao**
Shenzhen City
Guangdong 518057 (CN)

(74) Representative: **AWA Sweden AB**
P.O. Box 45086
104 30 Stockholm (SE)

(54) **DATA VERIFICATION METHOD, DATA TRANSMISSION METHOD, RELATED DEVICES, SYSTEM AND STORAGE MEDIUM**

(57) This application discloses a data verification method, including: receiving, fingerprint information of N data slices of to-be-sent data of a second device, wherein the N data slices are obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} data slice is obtained by updating second fingerprint information corresponding to an $(i-1)^{h}$ data slice with the ith data slice, and both N and i are integers greater than 1,receiving, the i^{th} data slice from the second device; updating, the received second fingerprint information with the i^{th} data slice to obtain third fingerprint information; and sending, data verification failure indication information to the second device in response to the third fingerprint information not matching the received first fingerprint information.

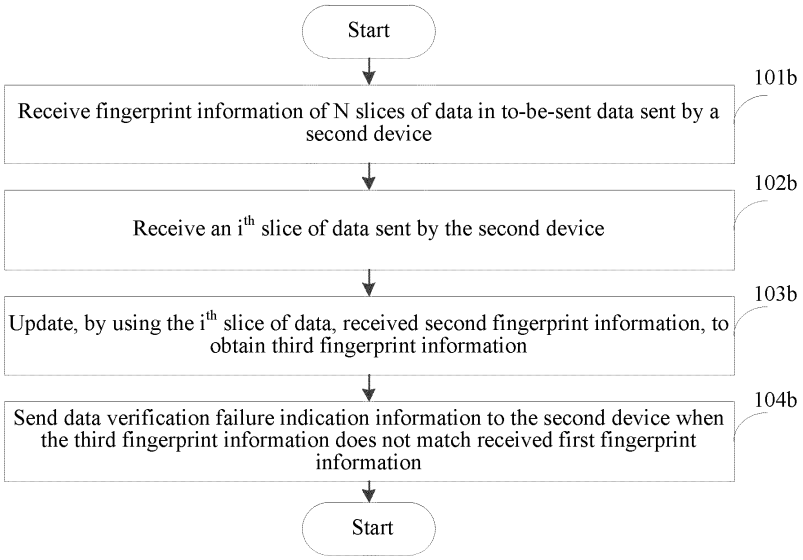

FIG. 1B

EP 3 606 007 A1

Description

RELATED APPLICATION

[0001] This application claims priority to Chinese Patent Application No. 201710170866.0, entitled "DATA VERIFICATION METHOD, DATA SENDING METHOD, RELATED APPARATUS, AND SYSTEM" filed with the Chinese Patent Office on March 21, 2017, which is incorporated by reference in its entirety.

FIELD OF THE TECHNOLOGY

[0002] This application relates to the field of computers, and in particular, to a data verification method, a data sending method, a data receiving apparatus, a data sending apparatus, a data transmission system, and a storage medium.

BACKGROUND OF THE DISCLOSURE

[0003] Cloud disks or cloud network disks are Internet storage tools. As products of Internet cloud technologies, the cloud disks provide services such as information storage, reading, and loading for enterprises and individuals through Internet, and are featured as secure, stable, and massive in storage.

[0004] With the development of electronic technologies and mobile Internet technologies, mobile electronic devices (particularly, intelligent mobile devices) have more powerful functions, and a user can do various things with the mobile electronic devices. Currently, a cloud network disk service may also provide a cloud storage function such as a file synchronization, backup, and sharing function for a mobile electronic device of a user end. Provided that the user installs a corresponding client on the mobile electronic device, the user and a server of the cloud network disk service may transmit data files to each other.

[0005] In the related art, a slice verification method is usually used for correctness verification in a data transmission process. That is, a data sending party sends a slice of data to a data receiving party, the data sending party first calculates a digest by using a digest algorithm and then transmits the data and the digest to the data receiving party, and then the data receiving party calculates again the received data by using the same digest algorithm for digest matching and comparison. For example, according to a verification method based on the Transmission Control Protocol (TCP) protocol, there is a checksum (a check code sum or a verification sum) field in a sent TCP header, and the correctness of the slice of data is determined through calculation, verification, and comparison.

SUMMARY

[0006] An embodiment of the present application discloses a data verification method, applied to a first device and including:

receiving fingerprint information of N data slices of to-be-sent data of a second device, wherein the N data slices are obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} data slice is obtained by updating second fingerprint information corresponding to an $(i-1)^{th}$ data slice with the i^{th} data slice, and both N and i are integers greater than 1;

receiving the i^{th} data slice from the second device;

updating the received second fingerprint information, with the i^{th} data slice to obtain third fingerprint information; and

sending data verification failure indication information to the second device in response to the third fingerprint information not matching the received first fingerprint information.

[0007] An embodiment of the present application discloses a data sending method, applied to a first device and including:

slicing to-be-sent data into M data slices;

calculating fingerprint information corresponding to each data slice, wherein, second fingerprint information corresponding to a $(j+1)^{th}$ data slice is obtained by updating third fingerprint information corresponding to a j^{th} data slice with the $(j+1)^{th}$ data slice, and both M and j being integers greater than 1; and

sending the fingerprint information corresponding to each data slice to a second device.

[0008] An embodiment of the present application further discloses a data verification apparatus, including a processor and a memory, the memory storing a computer-readable instruction ,the computer-readable instruction is configured to be executable by the processors to:

receive fingerprint information of N data slices of to-be-sent data of a second device, wherein the N data slices are obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} data slice is obtained by updating, second fingerprint information corresponding to an $(i-1)^{th}$ data slice with the i^{th} data slice, and both N and i are integers greater than 1;

receive the i^{th} data slice from the second device;

update, the received second fingerprint information with the i^{th} data slice, to obtain third fingerprint infor-

mation; and

send data verification failure indication information to the second device in response to the third fingerprint information not matching the received first fingerprint information.

[0009] An embodiment of the present application further discloses a data sending apparatus, including a processor and a memory, the memory storing a computer-readable instruction, the instruction is configured to be executable by the processors to:

slice to-be-sent data into N data slices ;

calculate fingerprint information corresponding to each data slice , wherein, second fingerprint information corresponding to a $(j+1)^{th}$ data slice is obtained by updating third fingerprint information corresponding to a j^{th} data slice with the $(j+1)^{th}$ data slice , and both M and j being integers greater than 1; and

send the fingerprint information corresponding to each data slice to a second device.

[0010] An embodiment of the present application further discloses a data transmission system, including the data sending apparatus and the data verification apparatus described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] To describe the technical solutions in the embodiments of this application or in the existing technology more clearly, the following briefly introduces the accompanying drawings for describing the embodiments or the existing technology. Apparently, the accompanying drawings in the following description show merely some embodiments of this application, and a person of ordinary skill in the art may still derive other drawings from the accompanying drawings without creative efforts.

FIG. 1A is a diagram of a scenario architecture of a data verification method or a data sending method according to an embodiment of this application.

FIG. 1B is a schematic flowchart of a data transmission method according to an embodiment of this application.

FIG. 1C is a schematic diagram of a process of calculating fingerprint information corresponding to to-be-sent data according to an embodiment of this application.

FIG. 2 is a schematic flowchart of a data transmission method according to an embodiment of this application.

FIG. 3 is a schematic diagram of a principle of calculating fingerprint information by slices by a sending party according to an embodiment of this application.

FIG. 4 is a schematic diagram of a principle of a method of verifying accumulated slices by a receiving party according to an embodiment of this application.

FIG. 5A is a schematic structural diagram of a data verification apparatus according to an embodiment of this application.

FIG. 5B is a schematic structural diagram of a data verification apparatus according to an embodiment of this application.

FIG. 6 is a schematic structural diagram of another embodiment of a data verification apparatus according to this application.

FIG. 7 is a schematic structural diagram of another embodiment of a data verification apparatus according to this application.

FIG. 8 is a schematic structural diagram of a data sending apparatus according to an embodiment of this application.

FIG. 9 is a schematic structural diagram of another embodiment of a data sending apparatus according to this application.

FIG. 10 is a schematic structural diagram of another embodiment of a data sending apparatus according to this application.

DESCRIPTION OF EMBODIMENTS

[0012] Technical solutions in embodiments of this application are described below with reference to the accompanying drawings in the embodiments of this application.

[0013] FIG. 1A is a diagram of a scenario architecture or a system architecture of a data verification method or a data sending method according to an embodiment of this application. An electronic device 101 may establish a connection with a server 103 by using a network 102 for data exchange. Using a cloud network disk as an example, a user can transmit a data file to the server end 103 that provides a cloud network disk service provided that the user installs a client on the electronic device 101. For example, the user synchronizes and backs up data to the server 103, or downloads required data from the server 103. When the electronic device 101 synchronizes and backs up data to the server 103, the electronic device

101 is a sending party of the data, and the server 103 is a receiving party of the data. When the electronic device 101 downloads required data from the server 103, the electronic device 101 is a receiving party of the data, and the server 103 is a sending party of the data. This embodiment of this application describes in detail how the sending party sends data and how the receiving party verifies the data with reference to FIG. 1B to FIG. 4.

[0014] It should be noted that, the electronic device 101 in this embodiment of this application includes but is not limited to an electronic device or a terminal device such as a personal computer, an intelligent mobile terminal (such as a mobile phone, a mobile computer, or a tablet computer), a personal digital assistant (PDA), a smart television, a smartwatch, smartglasses, and a smart band.

[0015] FIG. 1B is a schematic flowchart of a data verification method in the system architecture diagram shown in FIG. 1A. As shown in FIG. 1B, the data verification method may be performed by a first device. The first device may be the electronic device 101 or the server 103 shown in FIG. 1A, or may be any computing device that needs to transmit data in another application scenario. The method may include the following steps:

Step 101b: Receive fingerprint information of N slices of data in to-be-sent data sent by a second device, the N slices of data being obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} slice of data being fingerprint information obtained by updating, by using the i^{th} slice of data, second fingerprint information corresponding to an $(i-1)^{h}$ slice of data, and both N and i being integers greater than 1.

Step 102b: Receive the i^{th} slice of data sent by the second device.

Step 103b: Update, by using the i^{th} slice of data, the received second fingerprint information, to obtain third fingerprint information.

Step 104b: Send data verification failure indication information to the second device when the third fingerprint information does not match the received first fingerprint information.

[0016] In some examples, the first device may receive a first slice of data in the to-be-sent data sent by the second device, and calculate fourth fingerprint information of the first slice of data; determine whether the fourth fingerprint information matches fifth fingerprint information corresponding to the received first slice of data; and send the data verification failure indication information to the second device when the fourth fingerprint information does not match the fifth fingerprint information.

[0017] In some examples, the first device may receive sixth fingerprint information that is sent by the second device and that corresponds to the to-be-sent data; determine, by using the sixth fingerprint information, whether the to-be-sent data is stored in a database; and send data transmission indication information to the second device when determining that the to-be-sent data is not stored. Specifically, if the to-be-sent data is already stored, the fingerprint information corresponding to the to-be-sent data is also correspondingly stored. Therefore, before the first slice of data sent by the second device is received, the sixth fingerprint information corresponding to the entire to-be-sent data sent by the second device is received. If it is determined that seventh fingerprint information the same as the sixth fingerprint information is stored, it is determined that the to-be-sent data corresponding to the sixth fingerprint information is stored.

[0018] In some examples, the fingerprint information includes a message digest calculated by using a secure hash algorithm (SHA), or a message digest calculated by using a message-digest algorithm (MD).

[0019] In some examples, when the first device needs to send second to-be-sent data, the first device may slice the second to-be-sent data into M slices of data; and calculate fingerprint information corresponding to each slice of data, where second fingerprint information corresponding to a $(j+1)^{th}$ slice of data in the M slices of data is fingerprint information obtained by updating, by using the $(j+1)^{th}$ slice of data, third fingerprint information corresponding to a j^{th} slice of data, and both M and j are integers greater than 1; and send the fingerprint information corresponding to each slice of data to a third device. A value of M is determined by a size of the to-be-sent data and a used fingerprint calculation method.

[0020] In some examples, the first device may use an intermediate result of a process of calculating fingerprint information corresponding to the entire second to-be-sent data as the fingerprint information corresponding to each slice of data in the second to-be-sent data. That is, when the fingerprint information corresponding to each slice of data is calculated, the fingerprint information of the to-be-sent data may be calculated. The process of calculating the fingerprint information of the to-be-sent data may include:

calculating intermediate fingerprint information corresponding to a first slice of data in the M slices of data;

successively updating, by using the $(j+1)^{th}$ slice of data, intermediate fingerprint information corresponding to the j^{th} slice of data, to obtain intermediate fingerprint information corresponding to the $(j+1)^{th}$ slice of data; and

processing intermediate fingerprint information corresponding to an M^{th} slice of data to obtain the fingerprint information of the second to-be-sent data.

[0021] In the foregoing process of calculating the fingerprint information of the to-be-sent data, intermediate fingerprint information corresponding to slices of data other than the M^{th} slice of data is used as fingerprint information corresponding to the slices of data, and the fingerprint information corresponding to the second to-be-sent data is used as fingerprint information corresponding to the M^{th} slice of data.

[0022] FIG. 1C is a schematic diagram of a process of calculating the fingerprint information corresponding to the to-be-sent data. As shown in FIG. 1C, intermediate fingerprint information sha1 corresponding to a first slice of data 101c is first calculated, the intermediate fingerprint information sha1 is updated by using a second slice of data 102c to obtain intermediate fingerprint information sha2 corresponding to the second slice of data 102c, and the intermediate fingerprint information sha2 is updated by using a third slice of data 103c to obtain intermediate fingerprint information sha3 corresponding to the third slice of data 103c. According to this method, intermediate fingerprint information of each slice of data is calculated until the M^{th} slice of data. It should be noted that, after intermediate fingerprint information shaM of the M^{th} slice of data is obtained according to the foregoing method, the intermediate fingerprint information shaM of the M^{th} slice of data is updated by using information such as a length of the to-be-sent data to obtain the fingerprint information corresponding to the entire to-be-sent data.

[0023] In some examples, data verification failure indication information sent by the third device is received, where the data verification failure indication information includes information for indicating a k^{th} slice of data; and the k^{th} slice of data is sent to the third device according to the data verification failure indication information.

[0024] In some examples, after data transmission indication information sent by the third device is received, the M slices of data are sent to the third device according to the data transmission indication information.

[0025] During implementation of this embodiment of this application, fingerprint information that is of slices and that is prestored by a receiving party is verified, so that the fingerprint information of the slices of data is correlated to a sequence of the slices. Therefore, when a packet is tampered or forged or the slices are disordered, verification of a single slice of data cannot succeed, and as a result, a technical problem in the existing technology that a transmission error can be found only after an entire data file is downloaded is avoided, thereby avoiding fatal impact caused when a cloud network disk user uploads or downloads a large file. Moreover, according to this embodiment of this application, in a case in which whether a file is uploaded within seconds needs to be determined, time consumption for calculating and verifying the fingerprint information of the entire data and a calculation amount do not increase, so that verification efficiency is effectively ensured.

[0026] The following describes in detail the technical solutions of the data verification method and the data sending method provided in the embodiments of this application with reference to a schematic flowchart of a data transmission method provided in an embodiment of this application shown in FIG. 2. The technical solutions include the following steps:

Step S200: A sending party slices to-be-sent data into N slices of data.

[0027] In some examples, the sending party of the data may slice large data into N slices or N blocks for transmission. For example, a size of each sliced block or slice may be defined as 512 KB. It should be noted that, the sending party may be an electronic device on a user side, or may be a server on a network side. This is not limited herein.

[0028] Step S202: The sending party calculates fingerprint information corresponding to each slice of data.

[0029] In some example, slices of data have an order, ranging from a first slice to an N^{th} slice. When fingerprint information corresponding to the first slice of data is calculated according to this embodiment of this application, specifically, the fingerprint information may be obtained by calculating the first slice of data by using a corresponding fingerprint calculation algorithm. When fingerprint information corresponding to a $(j+1)^{th}$ slice of data is calculated, specifically, the $(j+1)^{th}$ slice of data may be updated to fingerprint information corresponding to a j^{th} slice of data to obtain updated data, and then the fingerprint information is obtained by calculating the updated data by using the corresponding fingerprint calculation algorithm. j is greater than or equal to 1, and less than or equal to N-1. That is, actually, when the fingerprint information corresponding to the $(j+1)^{th}$ slice of data is calculated, the fingerprint information may also be obtained by calculating accumulated data that is obtained after the first slice of data is accumulated to the $(j+1)^{th}$ slice of data.

[0030] FIG. 3 is a schematic diagram of a principle of calculating fingerprint information by slices by a sending party according to an embodiment of this application. For example, fingerprint information corresponding to a second slice of data is fingerprint information obtained by updating the second slice of data to fingerprint information corresponding to a first slice of data to obtain updated data, and then calculating the updated data; or fingerprint information obtained by calculating accumulated data that is obtained by adding the first slice of data to the second slice of data. For another example, fingerprint information corresponding to a tenth slice of data is fingerprint information obtained by updating the tenth slice of data to fingerprint information corresponding to a ninth slice of data to obtain updated data, and then calculating the updated data; or fingerprint information obtained by calculating accumulated data that is obtained by accumulating the first slice of data to the tenth slice of data.

[0031] Fingerprint information that corresponds to slices of data (rather than the first slice of data) and that is calculated according to the foregoing implementations is not determined only by content of separate slices of data, but is also correlated to fingerprint information of a pre-

vious slice of data, so that the fingerprint information of the slices of data is correlated to a sequence of the slices. Subsequently, in a corresponding verification process, a technical problem in the existing technology that when a packet is tampered or forged or the slices are disordered, verification of a single slice of data succeeds but verification of an entire data file fails, and as a result, a transmission error can be found only after the entire data file is downloaded is avoided, thereby avoiding fatal impact caused when a cloud network disk user uploads or downloads a large file.

[0032] It should be noted that, the fingerprint information in the embodiments of this application includes but is not limited to a message digest calculated by using an SHA, or a message digest calculated by using an MD. For example, the message digest is calculated by using SHA1, or the message digest is calculated by using MD4 or MD5. If a message digest calculated by an algorithm can represent feature information of data and has an update attribute, the message digest falls within the protection scope of the fingerprint information in this embodiment of this application.

[0033] Step S204: Send the fingerprint information corresponding to each slice of data to a receiving party.

[0034] Step S206: The receiving party receives the fingerprint information corresponding to each slice of data.

[0035] In some examples, after receiving the fingerprint information corresponding to each slice of data, the receiving party stores the fingerprint information corresponding to each slice of data for subsequent verification.

[0036] Step S208: The receiving party determines, by using the fingerprint information, whether target data is stored in a database.

[0037] In some examples, the received fingerprint information corresponding to each slice of data includes fingerprint information f corresponding to entire data. For example, in an implementation of calculating the fingerprint information in step S202, fingerprint information corresponding to a last slice of data (that is, an N^{th} slice of data) is exactly the fingerprint information f corresponding to the entire data. Therefore, if it is determined, according to the fingerprint information f, that the target data is stored in the database, where fingerprint information g corresponding to the target data matches the fingerprint information f, step S210 is performed; or if it is determined, according to the fingerprint information f, that the target data is not stored in the database, step S212 is performed.

[0038] Step S210: The receiving party returns data transmission success indication information to the sending party.

[0039] In some examples, if the receiving party determines, according to the fingerprint information f, that the target data is stored in the database, in other words, it indicates that the database already stores entire data to be sent by the sending party, the receiving party may return or send data transmission success indication information (or data transmission complete indication information or the like) to the sending party. The indication information is used to indicate, to the sending party, that the entire data has been successfully transmitted or transmission of the entire data completes, but actually, the entire data does not need to be retransmitted. This makes a user feel that the entire data is successfully transmitted within seconds.

[0040] Step S212: The receiving party sends data transmission indication information to the sending party.

[0041] In some examples, if the receiving party determines, according to the fingerprint information f, that the target data is not stored in the database, in other words, it indicates that data to be sent by the sending party needs to be received, the data transmission indication information is used to instruct the sending party to send the data. Further, both of communication parties may negotiate with each other on transmitting data blocks by using a plurality of TCP physical links. Then, the data transmission indication information may include information such as a quantity of TCP physical links (that is, a quantity of channels), a data offset of each TCP physical link, and a size of each slice of data.

[0042] Step S214: The sending party receives the data transmission indication information.

[0043] Step S216: The sending party sends each slice of data to the receiving party according to the data transmission indication information.

[0044] In some examples, based on information such as the quantity of TCP physical links (the quantity of channels) in the data transmission indication information, and the data offset of each TCP physical link and the size of each slice of data, the sending party sends the slice of data to the receiving party.

[0045] Step S218: The receiving party receives an i^{th} slice of data sent by the sending party.

[0046] In some examples, when receiving a slice of data, the receiving party may verify the slice of data. i is greater than or equal to 1, and less than or equal to N.

[0047] Step S220: Update, when i is not equal to 1, the i^{th} slice of data to prestored fingerprint information a, to obtain updated data.

[0048] In some examples, when the received i^{th} slice of data is not a first slice of data, the receiving party updates the i^{th} slice of data to the fingerprint information a, to obtain the updated data. The fingerprint information a in this embodiment of this application is fingerprint information corresponding to a prestored $(i-1)^{h}$ slice of data in step S206.

[0049] Step S222: Calculate fingerprint information b of the updated data.

[0050] In some examples, the fingerprint calculation algorithm used by the receiving party is the same as the fingerprint calculation algorithm used by the sending party in calculating the fingerprint information of the slices of data, and the fingerprint information b of the updated data is calculated by using the fingerprint calculation algorithm.

[0051] Step S224: Determine whether the fingerprint

information b matches fingerprint information c corresponding to the prestored i^{th} slice of data.

[0052] In some examples, if it is determined that the fingerprint information b does not match the fingerprint information c, in other words, verification fails, step S230 is performed. If it is determined that the fingerprint information b matches the fingerprint information c, in other words, verification succeeds, corresponding processing may be continued to be performed. For example, slices of data and the like are continued to be received. This is not limited in this embodiment of this application.

[0053] Step S226: Calculate fingerprint information d of the i^{th} slice of data when i is equal to 1.

[0054] In some examples, when the received i^{th} slice of data is the first slice of data, fingerprint information d of the first slice of data is directly calculated by using an algorithm the same as that used by the sending party in calculating the fingerprint information of the slices of data.

[0055] Step S228: Determine whether the fingerprint information d matches prestored fingerprint information e corresponding to the i^{th} slice of data.

[0056] In some examples, if it is determined that the fingerprint information d does not match the fingerprint information e, in other words, verification fails, step S230 is performed. If it is determined that the fingerprint information d matches the fingerprint information e, in other words, verification succeeds, corresponding processing may be continued to be performed. For example, slices of data and the like are continued to be received. This is not limited in this embodiment of this application.

[0057] It should be noted that, details of calculating, by the receiving party, fingerprint information corresponding to slices of data are shown in FIG. 4. FIG. 4 is a schematic diagram of a principle of a method of verifying accumulated slices by the receiving party according to an embodiment of this application. For example, fingerprint information corresponding to a second slice of data is fingerprint information obtained by updating the second slice of data to fingerprint information corresponding to a first slice of data to obtain updated data, and then calculating the updated data. For another example, fingerprint information corresponding to a tenth slice of data is fingerprint information obtained by updating the tenth slice of data to fingerprint information corresponding to a ninth slice of data to obtain updated data, and then calculating the updated data.

[0058] Fingerprint information that corresponds to slices of data (rather than the first slice of data) and that is calculated according to the foregoing implementations is not determined only by content of separate slices of data, but is also correlated to fingerprint information of a previous slice of data, so that the fingerprint information of the slices of data is correlated to a sequence of the slices. In a verification process, a technical problem in the existing technology that when a packet is tampered or forged or the slices are disordered, verification of a single slice of data succeeds but verification of an entire data file fails, and as a result, a transmission error can be found only after the entire data file is downloaded is avoided, thereby avoiding fatal impact caused when a cloud network disk user uploads or downloads a large file.

[0059] Step S230: Send data verification failure indication information to the sending party.

[0060] In some examples, the data verification failure indication information is used to indicate that an error occurs during transmission performed by the sending party, and the entire data needs to be retransmitted or a slice of data corresponding to a verification error needs to be retransmitted.

[0061] Step S232: The sending party receives the data verification failure indication information sent by the receiving party, and retransmits the to-be-sent data according to the data verification failure indication information.

[0062] In some examples, the sending party retransmits, according to content indicated by the data verification failure indication information, the entire data or the slice of data corresponding to the verification error.

[0063] During implementation of this embodiment of this application, an i^{th} slice of data sent by a sending party is received, the i^{th} slice of data is updated to prestored fingerprint information a, to obtain updated data. The fingerprint information a is fingerprint information corresponding to an $(i-1)^{th}$ slice of data. Fingerprint information b of the updated data is calculated, and whether the fingerprint information b matches fingerprint information c corresponding to the prestored i^{th} slice of data is determined. When the fingerprint information b does not match the fingerprint information c, data verification failure indication information is sent to the sending party. Fingerprint information of slices is accumulated for verification, so that the fingerprint information of slices of data is correlated to a sequence of the slices. Therefore, when a packet is tampered or forged or the slices are disordered, verification of a single slice of data cannot succeed, and as a result, a technical problem in the existing technology that a transmission error can be found only after an entire data file is downloaded is avoided, thereby avoiding fatal impact caused when a cloud network disk user uploads or downloads a large file. Moreover, according to this embodiment of this application, in a case in which whether a file is uploaded within seconds needs to be determined, time consumption for calculating and verifying the fingerprint information of the entire data and a calculation amount do not increase, so that verification efficiency is effectively ensured.

[0064] For ease of better implementing the foregoing solutions in the embodiments of this application, this application further correspondingly provides a data verification apparatus, which is described in detail below with reference to the accompanying drawings.

[0065] FIG. 5A and FIG. 5B are schematic structural diagrams of a data verification apparatus according to an embodiment of this application. In some examples of this application, as shown in FIG. 5A, the data verification apparatus 50 may include:

a data receiving module 501, configured to receive fingerprint information of N slices of data in to-be-sent data sent by a second device, the N slices of data being obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} slice of data being fingerprint information obtained by updating, by using the i^{th} slice of data, second fingerprint information corresponding to an $(i-1)^{th}$ slice of data, and both N and i being integers greater than 1;

the data receiving module 501 being further configured to receive the i^{th} slice of data sent by the second device;

an update module 503, configured to update, by using the i^{th} slice of data, the received second fingerprint information, to obtain third fingerprint information; and

an information sending module 505, configured to send data verification failure indication information to the second device when the third fingerprint information does not match the received first fingerprint information.

[0066] In some examples, the data receiving module 501 is further configured to receive a first slice of data in the to-be-sent data sent by the second device, and calculate fourth fingerprint information of the first slice of data; the update module 503 is further configured to determine whether the fourth fingerprint information matches fifth fingerprint information corresponding to the received first slice of data; and the information sending module 505 is further configured to send the data verification failure indication information to the second device when the fourth fingerprint information does not match the fifth fingerprint information.

[0067] In some examples, the data receiving module 501 is further configured to receive sixth fingerprint information that is sent by the second device and that corresponds to the to-be-sent data; the update module 503 is further configured to determine, by using the sixth fingerprint information, whether the to-be-sent data is stored in a database; and the information sending module 505 is further configured to send data transmission indication information to the second device when it is determined that the to-be-sent data is not stored.

[0068] In some examples, the data verification apparatus 50 may further include a data slicing module 507, a fingerprint calculation module 509, and a fingerprint information sending module 511.

[0069] The data slicing module 507 may slice second to-be-sent data into M slices of data.

[0070] The fingerprint calculation module 509 may calculate fingerprint information corresponding to each slice of data, where second fingerprint information corresponding to a $(j+1)^{th}$ slice of data in the M slices of data is fingerprint information obtained by updating, by using the $(j+1)^{th}$ slice of data, third fingerprint information corresponding to a j^{th} slice of data, and both M and j are integers greater than 1.

[0071] The fingerprint information sending module 511 may send the fingerprint information corresponding to each slice of data to a third device.

[0072] In some other examples of this application, as shown in FIG. 5B, the data verification apparatus 50 may include a data receiving module 500, an update module 502, a calculation and determining module 504, and an information sending module 506.

[0073] The data receiving module 500 is configured to receive an i^{th} slice of data sent by a sending party, where the sending party slices to-be-sent data into N slices of data for sending, and i is greater than or equal to 1 and less than or equal to N.

[0074] The update module 502 is configured to update, when i is not equal to 1, the i^{th} slice of data to prestored fingerprint information a to obtain updated data, where the fingerprint information a is fingerprint information corresponding to an $(i-1)^{th}$ slice of data.

[0075] The calculation and determining module 504 is configured to: calculate fingerprint information b of the updated data, and determine whether the fingerprint information b matches fingerprint information c corresponding to the prestored i^{th} slice of data.

[0076] The information sending module 506 is configured to send data verification failure indication information to the sending party when the fingerprint information b does not match the fingerprint information c.

[0077] In some examples, the calculation and determining module 504 is further configured to: calculate, when i is equal to 1, fingerprint information d of the i^{th} slice of data; and determine whether the fingerprint information d matches fingerprint information e corresponding to the i^{th} slice of data.

[0078] The information sending module 506 is further configured to send the data verification failure indication information to the sending party when the fingerprint information d does not match the fingerprint information e.

[0079] Further, FIG. 6 is a schematic structural diagram of another embodiment of a data verification apparatus according to this application. The data verification apparatus 50 may include a data receiving module 500, an update module 502, a calculation and determining module 504, and an information sending module 506, and may further include a fingerprint information receiving module 508 and a data determining module 5010.

[0080] The fingerprint information receiving module 508 is configured to receive fingerprint information f that is sent by a sending party and that corresponds to the to-be-sent data, before the data receiving module 500 receives an i^{th} slice of data sent by the sending party.

[0081] The data determine module 5010 is configured to determine, by using the fingerprint information f, whether target data is stored in a database, where fingerprint information g corresponding to the target data

matches the fingerprint information f.

[0082] The information sending module 506 is further configured to send data transmission indication information to the sending party when it is determined that the target data is not stored.

[0083] In some examples, the fingerprint information in this embodiment of this application includes a message digest calculated by using an SHA, or a message digest calculated by using an MD.

[0084] Still further, FIG. 7 is a schematic structural diagram of another embodiment of a data verification apparatus according to this application. The data verification apparatus 70 may include at least one processor 701, for example, a CPU, at least one network interface 704, a user interface 703, a memory 705, at least one communications bus 702, and a display 706. The communications bus 702 is configured to implement connection communication between the components. The user interface 703 may include a touchscreen, and the like. Optionally, the network interface 704 may include a standard wired interface and a standard wireless interface (such as a Wi-Fi interface). The memory 705 may be a high-speed RAM memory, or may be a non-volatile memory, for example, at least one magnetic disk memory. The memory 705 includes a flash in this embodiment of this application. Optionally, the memory 705 may be at least one storage system located remotely from the foregoing processor 701. As shown in FIG. 7, the memory 705, a computer storage medium, may include an operating system, a network communications module, a user interface module, and a data verification program.

[0085] In the data verification apparatus 70 shown in FIG. 7, the processor 701 may be configured to: invoke the data verification program stored in the memory 705, and perform processing operations in the embodiments of this application when a computing device receives data. For example, the processor 701 is capable of:

receiving, by using the network interface 704, an i^{th} slice of data sent by a sending party, where the sending party slices to-be-sent data into N slices of data for sending; and i is greater than or equal to 1, and less than or equal to N;

updating, when i is not equal to 1, the i^{th} slice of data to prestored fingerprint information a to obtain updated data, where the fingerprint information a is fingerprint information corresponding to an $(i-1)^{th}$ slice of data;

calculating fingerprint information b of the updated data, and determining whether the fingerprint information b matches fingerprint information c corresponding to the prestored i^{th} slice of data; and

sending data verification failure indication information to the sending party by using the network interface 704 when the fingerprint information b does not match the fingerprint information c.

[0086] In some examples, after receiving, by using the network interface 704, the i^{th} slice of data sent by the sending party, the processor 701 is further capable of:

calculating fingerprint information d of the i^{th} slice of data when i is equal to 1;

determining whether the fingerprint information d matches prestored fingerprint information e corresponding to the i^{th} slice of data; and

sending data verification failure indication information to the sending party by using the network interface 704 when the fingerprint information d does not match the fingerprint information e.

[0087] In some examples, before receiving, by using the network interface 704, the i^{th} slice of data sent by the sending party, the processor 701 is further capable of performing the following steps:

receiving, by using the network interface 704, fingerprint information f that is sent by the sending party and that corresponds to the to-be-sent data;

determining, by using the fingerprint information f, whether target data is stored in a database, where fingerprint information g corresponding to the target data matches the fingerprint information f; and

sending data transmission indication information to the sending party by using the network interface 704 when determining that the target data is not stored.

[0088] In some examples, the fingerprint information includes a message digest calculated by using an SHA, or a message digest calculated by using an MD.

[0089] It should be noted that, for functions of the modules in the data verification apparatus 50 or the data verification apparatus 70 in the embodiments of this application, refer to a specific implementation of any embodiment of FIG. 2 to FIG. 4 in the foregoing method embodiments, and details are not repeatedly described. The data verification apparatus 50 or the data verification apparatus 70 may include, but not limited to, an electronic device or a terminal device such as a personal computer, and an intelligent mobile terminal (such as a mobile phone, a mobile computer, or a tablet computer).

[0090] For ease of better implementing the foregoing solutions in the embodiments of this application, this application further correspondingly provides a data sending apparatus, which is described in detail below with reference to the accompanying drawings:

[0091] FIG. 8 is a schematic structural diagram of a data sending apparatus according to an embodiment of this application. The data sending apparatus 80 may in-

clude a data slicing module 800, a fingerprint calculation module 802, and a fingerprint information sending module 804.

[0092] The data slicing module 800 is configured to slice to-be-sent data into N slices of data.

[0093] The fingerprint calculation module 802 is configured to calculate fingerprint information corresponding to each slice of data, where fingerprint information corresponding to a first slice of data is fingerprint information obtained by calculating the first slice of data; fingerprint information corresponding to a $(j+1)^{th}$ slice of data is fingerprint information obtained by calculating updated data; and the updated data is data obtained after updating the $(j+1)^{th}$ slice of data to fingerprint information corresponding to a j^{th} slice of data, where j is greater than or equal to 1, and less than or equal to N-1.

[0094] The fingerprint information sending module 804 is configured to send the fingerprint information corresponding to each slice of data to a receiving party.

[0095] In some examples, FIG. 9 is a schematic structural diagram of another embodiment of a data sending apparatus according to this application. The data sending apparatus 80 includes a data slicing module 800, a fingerprint calculation module 802, and a fingerprint information sending module 804, and may further include an information receiving module 806, a data sending module 808, and a retransmission module 8010.

[0096] The information receiving module 806 is configured to receive data transmission indication information sent by a receiving party, after the fingerprint information sending module 804 sends fingerprint information corresponding to each slice of data to the receiving party.

[0097] The data sending module 808 is configured to send each slice of data to the receiving party according to the data transmission indication information.

[0098] Further, the information receiving module 806 is further configured to receive data verification failure indication information sent by the receiving party, after the data sending module 808 sends each slice of data to the receiving party.

[0099] The retransmission module 8010 is configured to retransmit the to-be-sent data according to the data verification failure indication information.

[0100] Still further, FIG. 10 is a schematic structural diagram of another embodiment of a data sending apparatus according to this application. The data sending apparatus 100 may include at least one processor 1001, for example, a CPU, at least one network interface 1004, a user interface 1003, a memory 1005, at least one communications bus 1002, and a display 1006. The communications bus 1002 is configured to implement connection communication between the components. The user interface 1003 may include a touchscreen, and the like. Optionally, the network interface 1004 may include a standard wired interface and a standard wireless interface (such as a Wi-Fi interface). The memory 1005 may be a high-speed RAM memory, or may be a non-volatile memory, for example, at least one magnetic disk memory. The memory 1005 includes a flash in this embodiment of this application. Optionally, the memory 1005 may be at least one storage system located remotely from the foregoing processor 1001. As shown in FIG. 10, the memory 1005, a computer storage medium, may include an operating system, a network communications module, a user interface, and a data sending program.

[0101] In the data sending apparatus 100 shown in FIG. 10, the processor 1001 may be configured to: invoke the data sending program stored in the memory 1005, and perform processing operations in the embodiments of this application when a computing device sends data. For example, the processor 1001 is capable of:

slicing to-be-sent data into N slices of data;

calculating fingerprint information corresponding to each slice of data, where fingerprint information corresponding to a first slice of data is fingerprint information obtained by calculating the first slice of data; fingerprint information corresponding to a $(j+1)^{th}$ slice of data is fingerprint information obtained by calculating updated data; and the updated data is data obtained after updating the $(j+1)^{th}$ slice of data to fingerprint information corresponding to a j^{th} slice of data, where j is greater than or equal to 1, and less than or equal to N-1; and

sending the fingerprint information corresponding to each slice of data to the receiving party by using the network interface 1004.

[0102] In some examples, when a memory in an apparatus stores both the data verification program shown in FIG. 7 and the data sending program shown in FIG. 10, the apparatus has the functions of both the data verification apparatus shown in FIG. 7 and the data sending apparatus shown in FIG. 10.

[0103] In some examples, after sending the fingerprint information corresponding to each slice of data to the receiving party by using the network interface 1004, the processor 1001 may further be capable of performing the following step:

sending each slice of data to the receiving party by using the network interface 1004 according to data transmission indication information, after receiving the data transmission indication information sent by the receiving party by using the network interface 1004.

[0104] In some examples, after sending each slice of data to the receiving party by using the network interface 1004, the processor 1001 may further be capable of performing the following steps:

receiving data verification failure indication information sent by the receiving party by using the network interface 1004; and

retransmitting the to-be-sent data by using the net-

work interface 1004 according to the data verification failure indication information.

[0105] It should be noted that, for functions of the modules in the data sending apparatus 80 or the data sending apparatus 100 in the embodiments of this application, refer to a specific implementation of any embodiment of FIG. 2 to FIG. 4 in the foregoing method embodiments, and details are not repeatedly described. The data sending apparatus 80 or the data sending apparatus 100 may include, but not limited to, an electronic device or a terminal device such as a personal computer, and an intelligent mobile terminal (such as a mobile phone, a mobile computer, or a tablet computer).

[0106] For ease of better implementing the solutions in the embodiments of this application, this application further correspondingly provides a data transmission system. The data transmission system may include the data verification apparatus in FIG. 5 to FIG. 7, and the data sending apparatus in FIG. 8 to FIG. 10. For details as to how the data transmission system transmits data, refer to a specific implementation of any embodiment of FIG. 2 to FIG. 4 in the method embodiments, and details are not repeatedly described.

[0107] During implementation of this embodiment of this application, an i^{th} slice of data sent by a sending party is received, the i^{th} slice of data is updated to prestored fingerprint information a, to obtain updated data. The fingerprint information a is fingerprint information corresponding to an $(i-1)^{th}$ slice of data. Fingerprint information b of the updated data is calculated, and whether the fingerprint information b matches fingerprint information c corresponding to the prestored i^{th} slice of data is determined. When the fingerprint information b does not match the fingerprint information c, data verification failure indication information is sent to the sending party. Fingerprint information of slices is accumulated for verification, so that the fingerprint information of slices of data is correlated to a sequence of the slices. Therefore, when a packet is tampered or forged or the slices are disordered, verification of a single slice of data cannot succeed, and as a result, a technical problem in the existing technology that a transmission error can be found only after an entire data file is downloaded is avoided, thereby avoiding fatal impact caused when a cloud network disk user uploads or downloads a large file. Moreover, according to this embodiment of this application, in a case in which whether a file is uploaded within seconds needs to be determined, time consumption for calculating and verifying the fingerprint information of the entire data and a calculation amount do not increase, so that verification efficiency is effectively ensured.

[0108] A person of ordinary skill in the art may understand that all or some of the processes of the methods in the embodiments may be implemented by a computer program instructing relevant hardware. The program may be stored in a computer readable storage medium. When the program is run, the processes of the embodiments of the foregoing methods may be included. The foregoing storage medium may be a magnetic disk, an optical disc, a read-only memory (ROM), or a random access memory (RAM).

[0109] What is disclosed above is merely a preferred embodiment of the embodiments of this application, and certainly is not intended to limit the protection scope of this application. Therefore, equivalent variations made in accordance with the claims of this application shall fall within the scope of this application.

Claims

1. A data verification method, applied to a first device, comprising:

   receiving, fingerprint information of N data slices of to-be-sent data of a second device, wherein the N data slices are obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} data slice is obtained by updating second fingerprint information corresponding to an $(i-1)^{th}$ data slice with the i^{th} data slice, and both N and i are integers greater than 1;
   receiving, the i^{th} data slice from the second device;
   updating, the received second fingerprint information with the i^{th} data slice to obtain third fingerprint information; and
   sending, data verification failure indication information to the second device in response to the third fingerprint information not matching the received first fingerprint information.

2. The method according to claim 1, further comprising:

   receiving, a first data slice of the to-be-sent data from the second device;
   calculating, fourth fingerprint information of the first data slice of the to-be-sent data;
   determining, whether the fourth fingerprint information matches fifth fingerprint information corresponding to the received first data slice of the to-be-sent data; and
   sending the data verification failure indication information to the second device in response to the fourth fingerprint information not matching the fifth fingerprint information.

3. The method according to claim 2, further comprising:

   receiving, sixth fingerprint information corresponding to the to-be-sent data from the second device;
   determining, whether the to-be-sent data is stored in a database according to the sixth fin-

gerprint information; and
sending, data transmission indication information to the second device in response to determining that the to-be-sent data is not stored.

4. The method according to any one of claims 1 to 3, wherein the fingerprint information comprises a message digest calculated by a secure hash algorithm SHA, or a message digest calculated by a message-digest algorithm MD.

5. The method according to claim 1, further comprising:

slicing second to-be-sent data into M data slices ;
calculating, fingerprint information corresponding to each of the M data slices , wherein second fingerprint information corresponding to a $(j+1)^{th}$ data slice of in the M data slices is obtained by updating third fingerprint information corresponding to a j^{th} data slice with the $(j+1)^{th}$ data slice, and both M and j are integers greater than 1; and
sending the fingerprint information corresponding to the each data slice to a third device.

6. The method according to claim 5, wherein the calculating fingerprint information corresponding to each of the M data slices comprises:

calculating fingerprint information of the second to-be-sent data; and
the calculating fingerprint information of the second to-be-sent data comprises:

calculating, intermediate fingerprint information corresponding to a first data slice in the M data slices ;
successively updating, intermediate fingerprint information corresponding to the j^{th} data slice with the $(j+1)^{th}$ data slice, to obtain intermediate fingerprint information corresponding to the $(j+1)^{th}$ data slice;
processing intermediate fingerprint information corresponding to an M^{th} data slice to obtain the fingerprint information of the second to-be-sent data;

determining, intermediate fingerprint information corresponding to each data slice other than the M^{th} data slice as the fingerprint information corresponding to each data slice ; and
using, the fingerprint information of the second to-be-sent data as fingerprint information corresponding to the M^{th} data slice .

7. The method according to claim 5, wherein the method further comprises:

receiving, from the third device, the data verification failure indication information, wherein the data verification failure indication information comprises information indicating a k^{th} data slice ;
sending, the k^{th} data slice to the third device according to the data verification failure indication information.

8. The method according to claim 5, further comprising:
sending, the M data slices to the third device according to the data transmission indication information, after receiving data transmission indication information from the third device.

9. A data sending method, applied to a first device and comprising:

slicing to-be-sent data into N data slices ;
calculating, fingerprint information corresponding to each data slice, wherein, second fingerprint information corresponding to a $(j+1)^{th}$ data slice is obtained by updating third fingerprint information corresponding to a j^{th} data slice with the $(j+1)^{th}$ data slice, and both M and j being integers greater than 1; and
sending the fingerprint information corresponding to each slice of data to a second device.

10. The method according to claim 9, wherein, the calculating fingerprint information corresponding to each data slice comprises:

calculating, fingerprint information of the second to-be-sent data; and
wherein, the calculating fingerprint information of the second to-be-sent data comprises:

calculating, intermediate fingerprint information corresponding to a first data slice of the to-be-sent data;
updating, intermediate fingerprint information corresponding to the j^{th} data slice of the to-be-sent data with the $(j+1)^{th}$ data slice of the to-be-sent data successively, to obtain intermediate fingerprint information corresponding to the $(j+1)^{th}$ data slice of the to-be-sent data;
processing, intermediate fingerprint information corresponding to an M^{th} data slice of the to-be-sent data to obtain the fingerprint information of the second to-be-sent data;

determining, intermediate fingerprint information corresponding to each data slice of the to-be-sent data other than the M^{th} data slice of the to-be-sent data as the fingerprint information

corresponding to the each data slice of the to-be-sent data; and

using, the fingerprint information of the second to-be-sent data as fingerprint information corresponding to the M^{th} data slice of the to-be-sent data.

11. The method according to claim 9, further comprising:

sending, the M data slices of the to-be-sent data to the second device according to the data transmission indication information, after receiving data transmission indication information from the second device.

12. The method according to claim 9, further comprising:

receiving, data verification failure indication information from the second device, wherein, the data verification failure indication information comprises information indicating a k^{th} data slice; and

sending, the k^{th} data slice to the second device according to the data verification failure indication information.

13. A data verification apparatus, comprising a processor and a memory, the memory storing a computer-readable instruction, the computer-readable instruction is configured to be executable by the processors to:

receive fingerprint information of N data slices of to-be-sent data of a second device, wherein the N data slices are obtained by slicing the to-be-sent data; and in the fingerprint information, first fingerprint information corresponding to an i^{th} data slice is obtained by updating second fingerprint information corresponding to an $(i-1)^{th}$ data slice with the i^{th} data slice, and both N and i are integers greater than 1;

receive the i^{th} data slice from the second device;

update the received second fingerprint information with the i^{th} data slice, to obtain third fingerprint information; and

send data verification failure indication information to the second device in response to the third fingerprint information not matching the received first fingerprint information.

14. The apparatus according to claim 13, wherein the instruction is capable of causing the processor to:

receive a first slice of data in the to-be-sent data sent by the second device, and calculate fourth fingerprint information of the first slice of data;

determine whether the fourth fingerprint information matches fifth fingerprint information corresponding to the received first slice of data; and

send the data verification failure indication information to the second device when the fourth fingerprint information does not match the fifth fingerprint information.

15. The apparatus according to claim 14, wherein the instruction is capable of causing the processor to:

receive sixth fingerprint information that is sent by the second device and that corresponds to the to-be-sent data, before receiving the first slice of data sent by the second device;

determine, by using the sixth fingerprint information, whether the to-be-sent data is stored in a database; and

send data transmission indication information to the second device when determining that the to-be-sent data is not stored.

16. The apparatus according to claim 13, wherein the instruction is capable of causing the processor to:

slice second to-be-sent data into M slices of data;

calculate fingerprint information corresponding to each of the M slices of data, wherein second fingerprint information corresponding to a $(j+1)^{th}$ slice of data in the M slices of data is fingerprint information obtained by updating, by using the $(j+1)^{th}$ slice of data, third fingerprint information corresponding to a j^{th} slice of data, and both M and j are integers greater than 1; and

send the fingerprint information corresponding to each slice of data to a third device.

17. The apparatus according to claim 16, wherein the instruction is capable of causing the processor to:

calculate fingerprint information of the second to-be-sent data; and

the calculating fingerprint information of the second to-be-sent data comprises:

calculating intermediate fingerprint information corresponding to a first slice of data in the M slices of data;

successively updating, by using the $(j+1)^{th}$ slice of data, intermediate fingerprint information corresponding to the j^{th} slice of data, to obtain intermediate fingerprint information corresponding to the $(j+1)^{th}$ slice of data;

processing intermediate fingerprint information corresponding to an M^{th} slice of data to obtain the fingerprint information of the second to-be-sent data;

determining intermediate fingerprint information corresponding to each slice of data other than the M^{th} slice of data as the fin-

gerprint information corresponding to the slice of data; and
using the fingerprint information of the second to-be-sent data as fingerprint information corresponding to the M^{th} slice of data.

18. A data sending apparatus, comprising a processor and a memory, the memory storing a computer-readable instruction, the computer-readable instruction is configured to be executable by the processors to:

slice to-be-sent data into N data slices;
calculate fingerprint information corresponding to each data slice, wherein, second fingerprint information corresponding to a $(j+1)^{th}$ data slice is obtained by updating third fingerprint information corresponding to a j^{th} data slice with the $(j+1)^{th}$ data slice, and both M and j being integers greater than 1; and
send the fingerprint information corresponding to each data slice to a second device.

19. The apparatus according to claim 18, wherein the instruction is capable of causing the processor to:

calculate fingerprint information of the second to-be-sent data; and
the calculating fingerprint information of the second to-be-sent data comprises:

calculating intermediate fingerprint information corresponding to a first slice of data in the M slices of data;
successively updating, by using the $(j+1)^{th}$ slice of data, intermediate fingerprint information corresponding to the j^{th} slice of data, to obtain intermediate fingerprint information corresponding to the $(j+1)^{th}$ slice of data;
processing intermediate fingerprint information corresponding to an M^{th} slice of data to obtain the fingerprint information of the second to-be-sent data;

determining intermediate fingerprint information corresponding to each slice of data other than the M^{th} slice of data as the fingerprint information corresponding to the slice of data; and
using the fingerprint information of the second to-be-sent data as fingerprint information corresponding to the M^{th} slice of data.

20. A non-volatile computer-readable storage medium, storing a computer-readable instruction, the instruction is configured to be executable by the processors to perform the method according to any one of claims 1 to 12.

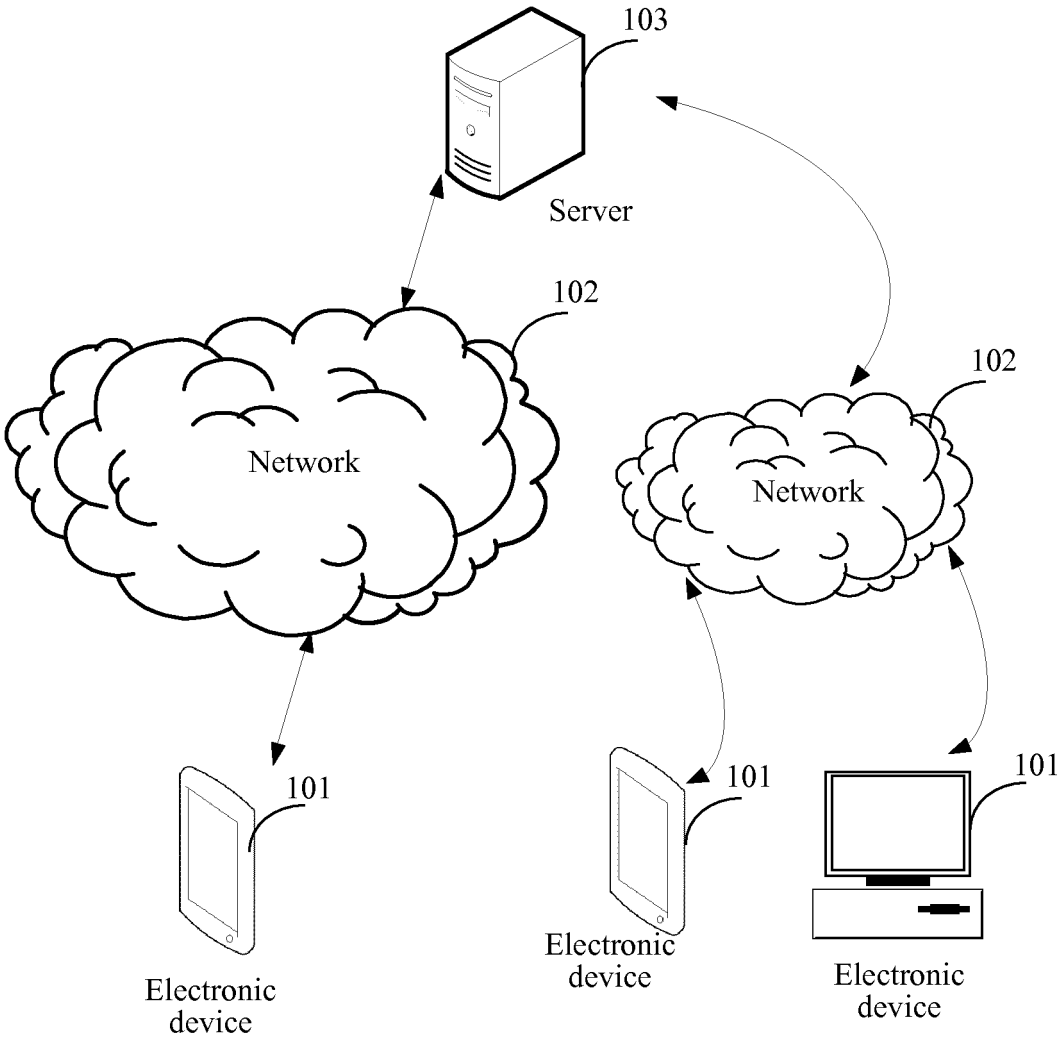
103
Server
102
Network
102
Network
101
Electronic device
101
Electronic device
101
Electronic device

FIG. 1A

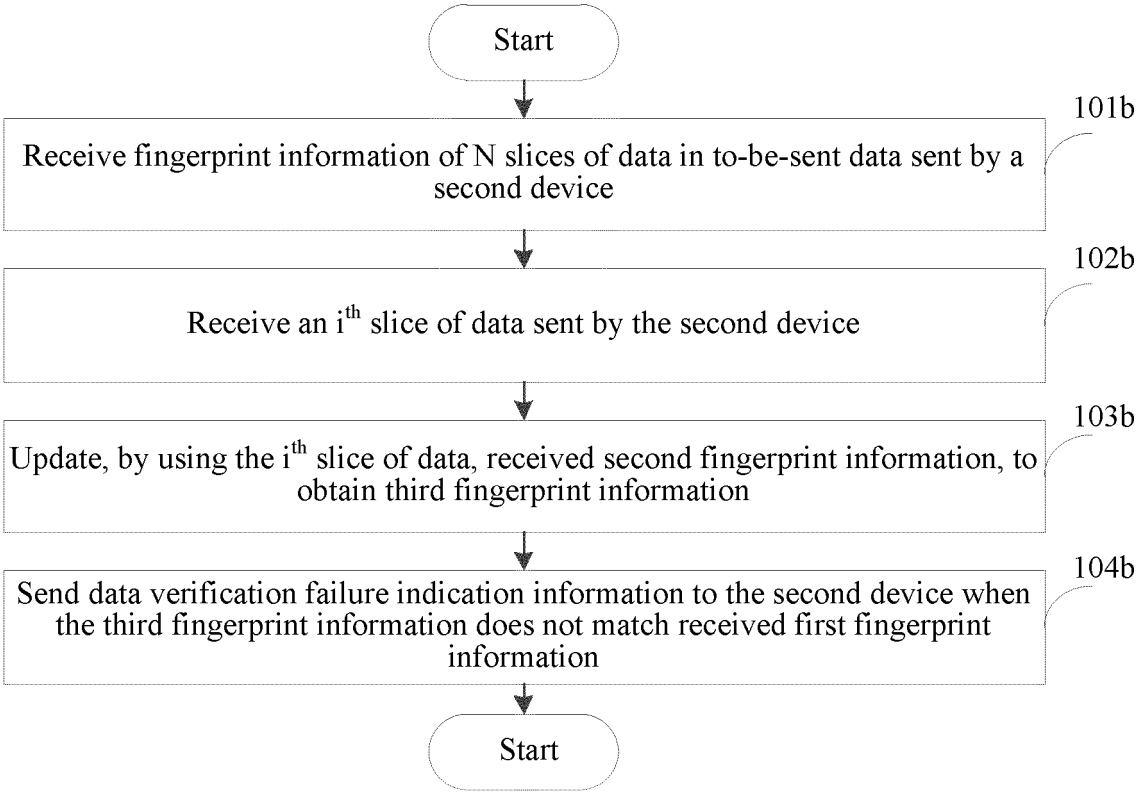
Start
Receive fingerprint information of N slices of data in to-be-sent data sent by a second device
101b
Receive an i^th slice of data sent by the second device
102b
Update, by using the i^th slice of data, received second fingerprint information, to obtain third fingerprint information
103b
Send data verification failure indication information to the second device when the third fingerprint information does not match received first fingerprint information
104b
Start

FIG. 1B

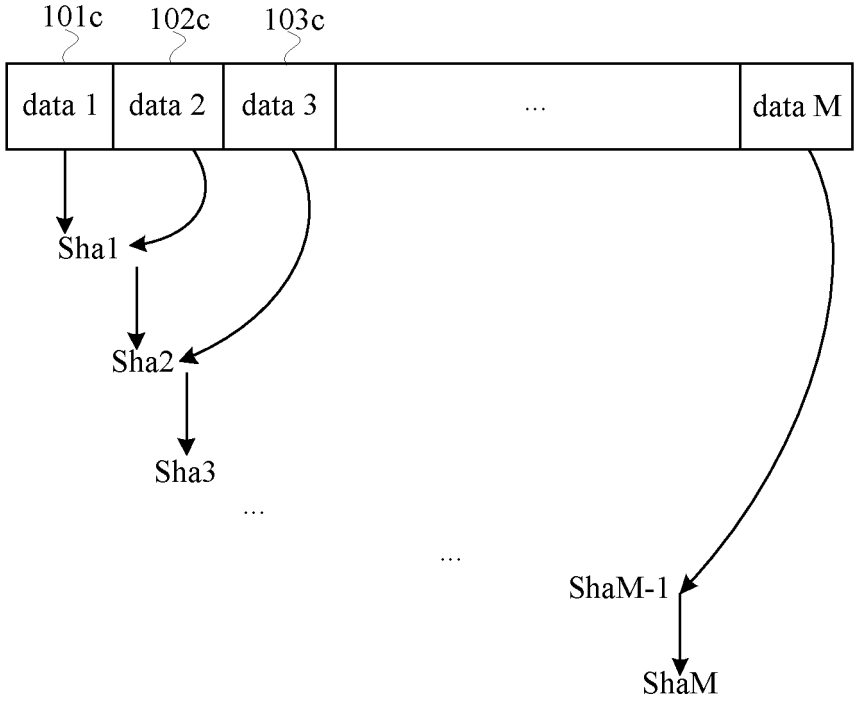
101c
102c
103c
data 1
data 2
data 3
...
data M
Sha1
Sha2
Sha3
...
...
ShaM-1
ShaM

FIG. 1C

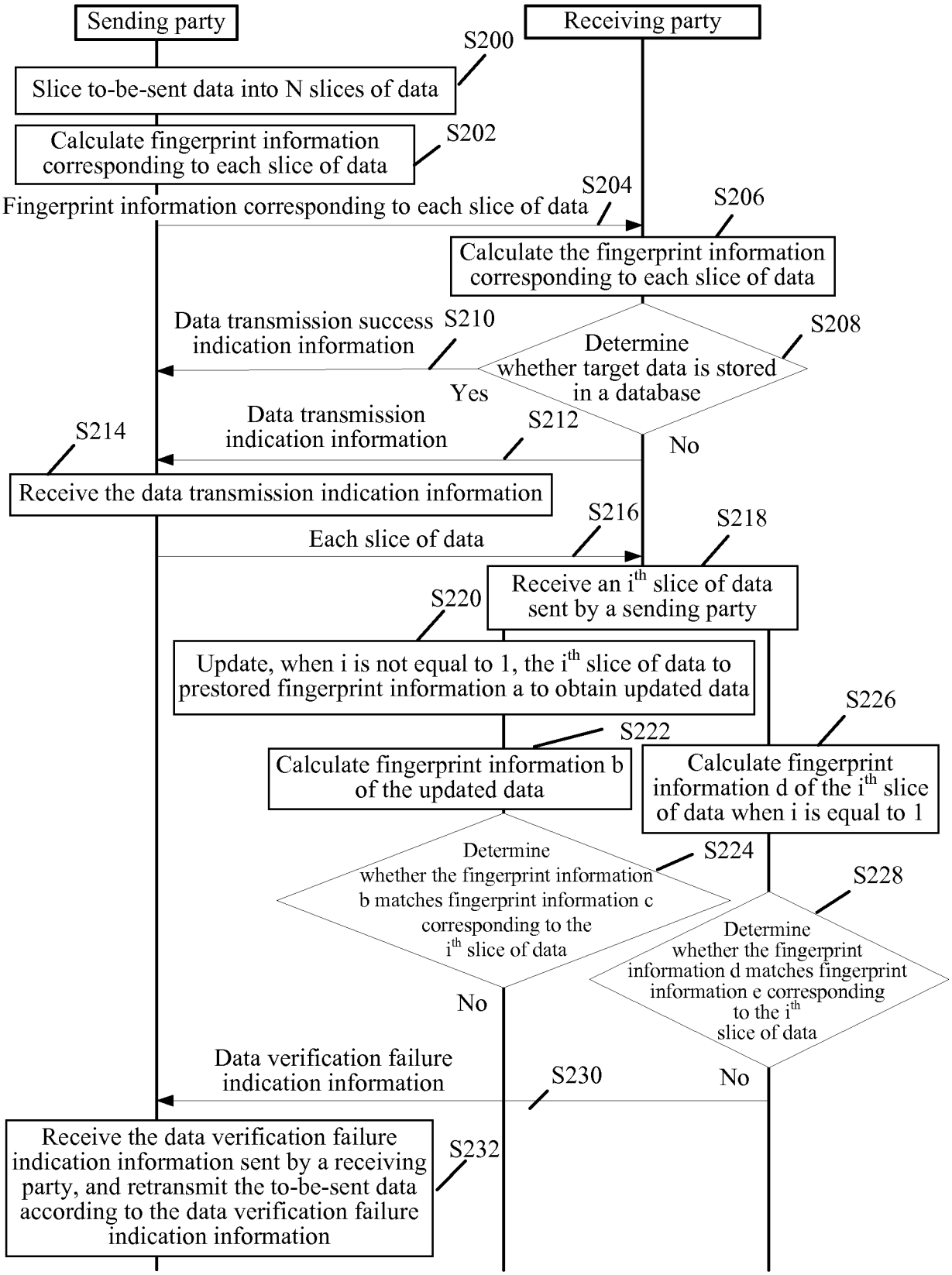
Sending party
Receiving party
S200
Slice to-be-sent data into N slices of data
Calculate fingerprint information corresponding to each slice of data
S202
Fingerprint information corresponding to each slice of data
S204
S206
Calculate the fingerprint information corresponding to each slice of data
Data transmission success indication information
S210
S208
Determine whether target data is stored in a database
Yes
No
Data transmission indication information
S212
S214
Receive the data transmission indication information
S216
Each slice of data
S218
Receive an i^th slice of data sent by a sending party
S220
Update, when i is not equal to 1, the i^th slice of data to prestored fingerprint information a to obtain updated data
S226
S222
Calculate fingerprint information b of the updated data
Calculate fingerprint information d of the i^th slice of data when i is equal to 1
Determine whether the fingerprint information b matches fingerprint information c corresponding to the i^th slice of data
S224
S228
Determine whether the fingerprint information d matches fingerprint information e corresponding to the i^th slice of data
No
No
Data verification failure indication information
S230
Receive the data verification failure indication information sent by a receiving party, and retransmit the to-be-sent data according to the data verification failure indication information
S232

FIG. 2

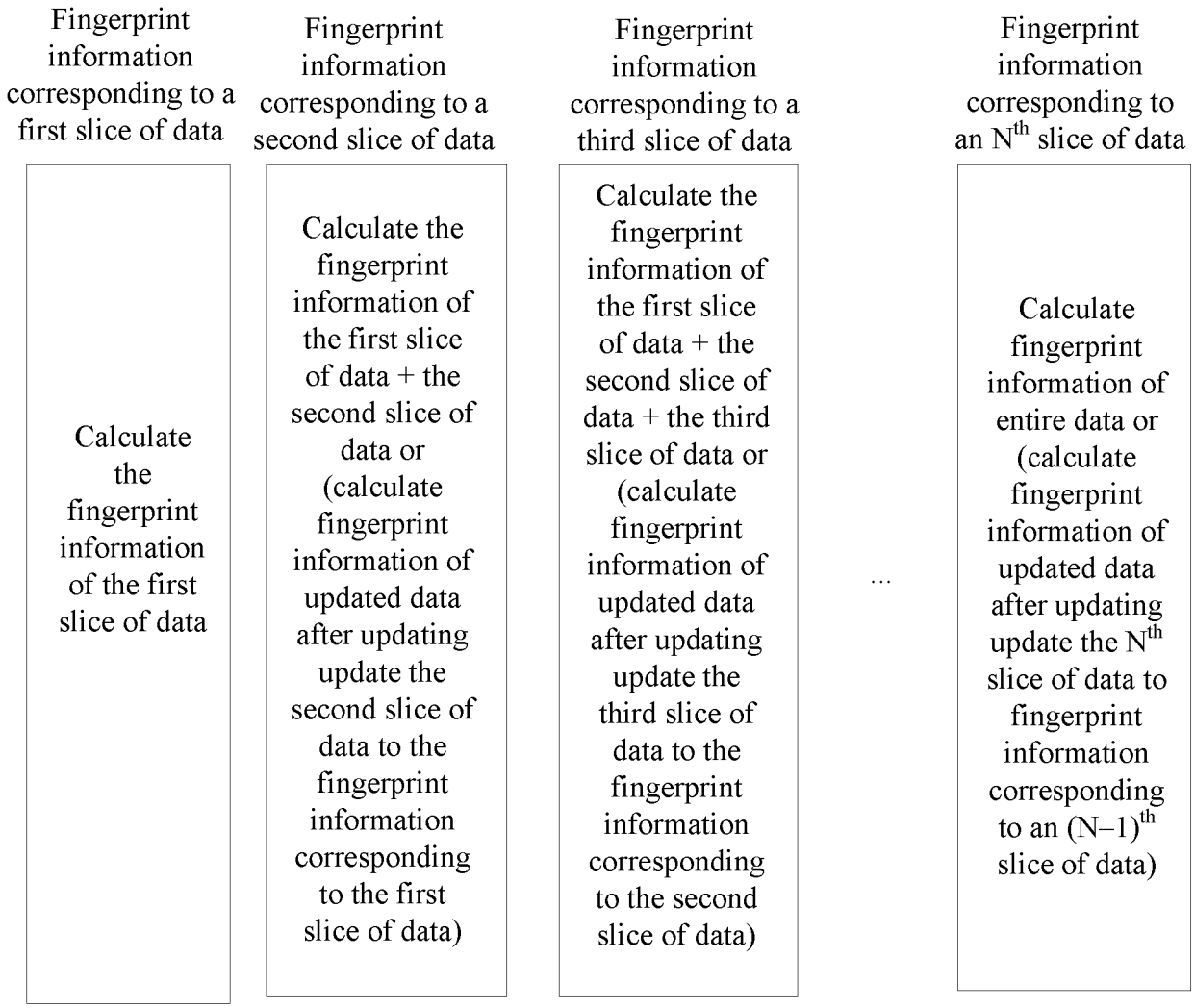
Fingerprint information corresponding to a first slice of data
Fingerprint information corresponding to a second slice of data
Fingerprint information corresponding to a third slice of data
Fingerprint information corresponding to an N^th slice of data
Calculate the fingerprint information of the first slice of data
Calculate the fingerprint information of the first slice of data + the second slice of data or (calculate fingerprint information of updated data after updating update the second slice of data to the fingerprint information corresponding to the first slice of data)
Calculate the fingerprint information of the first slice of data + the second slice of data + the third slice of data or (calculate fingerprint information of updated data after updating update the third slice of data to the fingerprint information corresponding to the second slice of data)
...
Calculate fingerprint information of entire data or (calculate fingerprint information of updated data after updating update the N^th slice of data to fingerprint information corresponding to an (N–1)^th slice of data)

FIG. 3

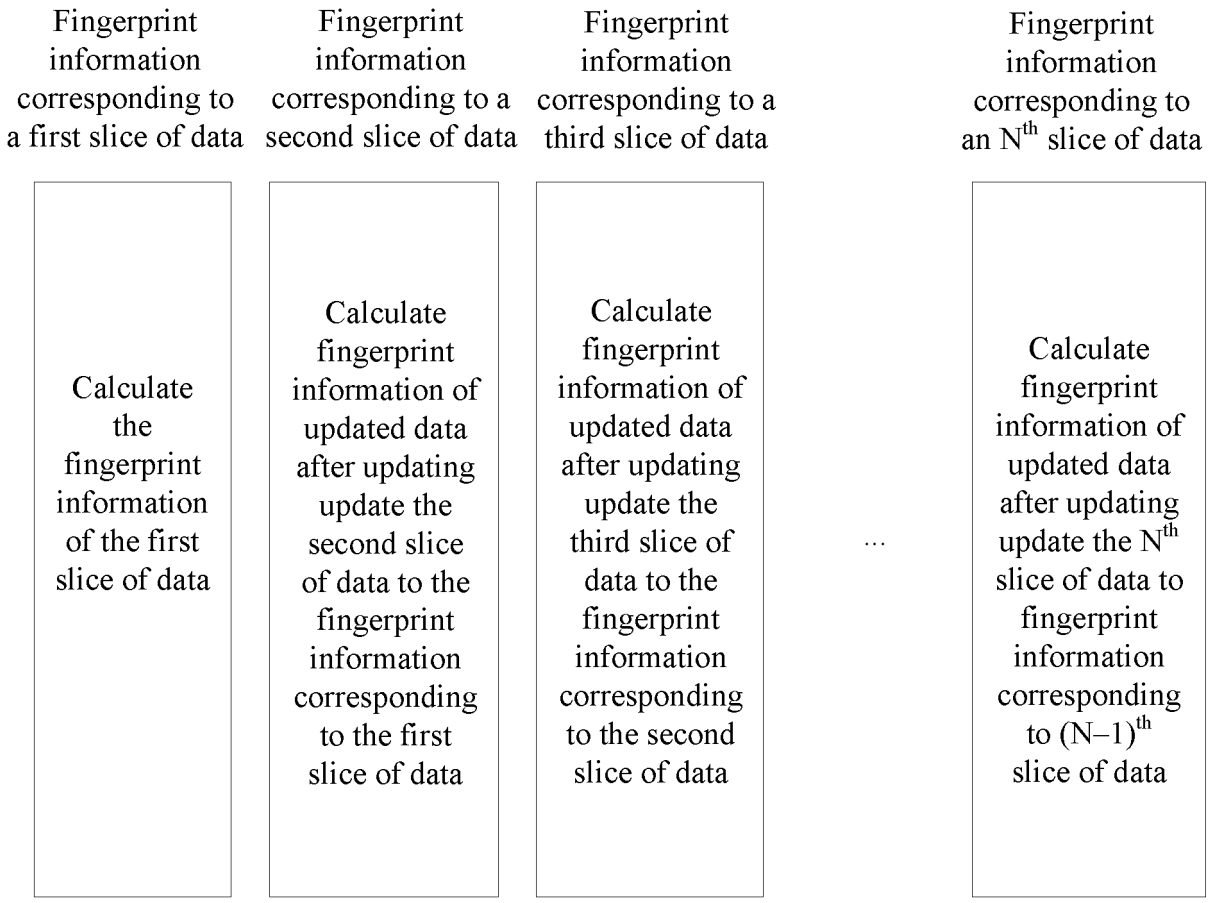
Fingerprint information corresponding to a first slice of data
Fingerprint information corresponding to a second slice of data
Fingerprint information corresponding to a third slice of data
Fingerprint information corresponding to an N^th slice of data
Calculate the fingerprint information of the first slice of data
Calculate fingerprint information of updated data after updating update the second slice of data to the fingerprint information corresponding to the first slice of data
Calculate fingerprint information of updated data after updating update the third slice of data to the fingerprint information corresponding to the second slice of data
...
Calculate fingerprint information of updated data after updating update the N^th slice of data to fingerprint information corresponding to (N–1)^th slice of data

FIG. 4

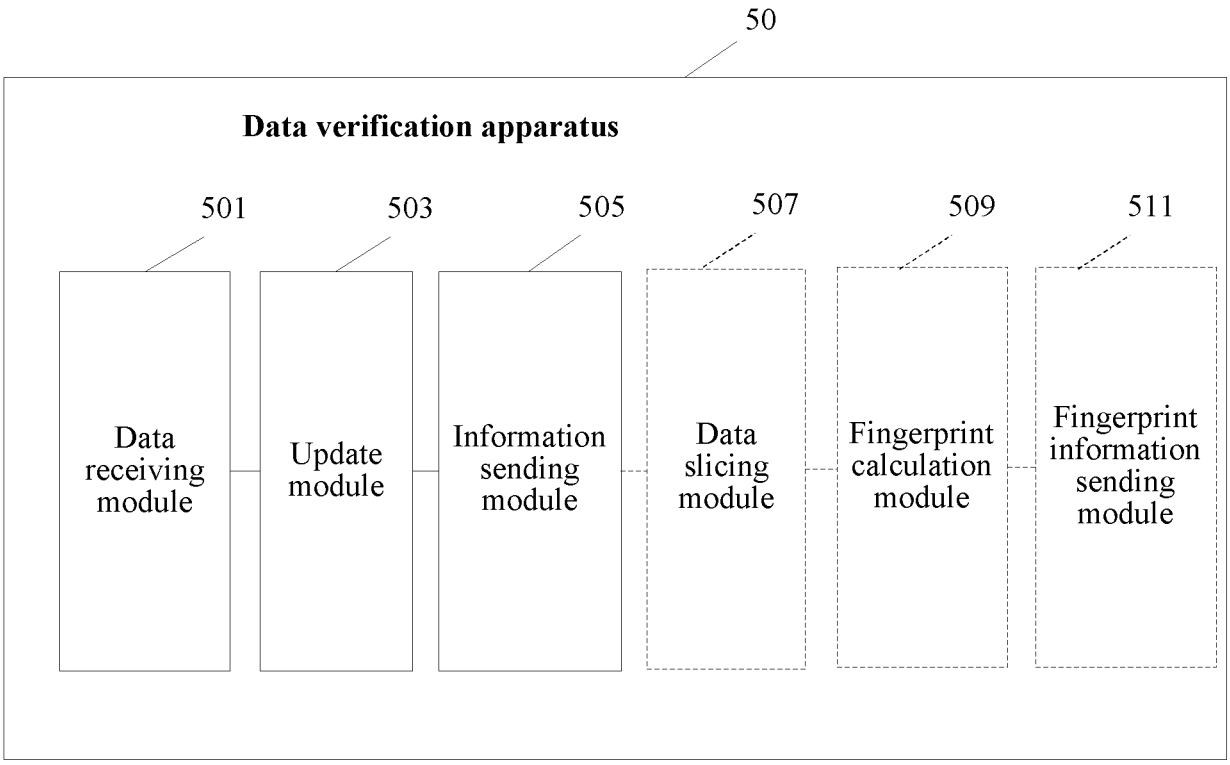
50
Data verification apparatus
501
503
505
507
509
511
Data receiving module
Update module
Information sending module
Data slicing module
Fingerprint calculation module
Fingerprint information sending module

FIG. 5A

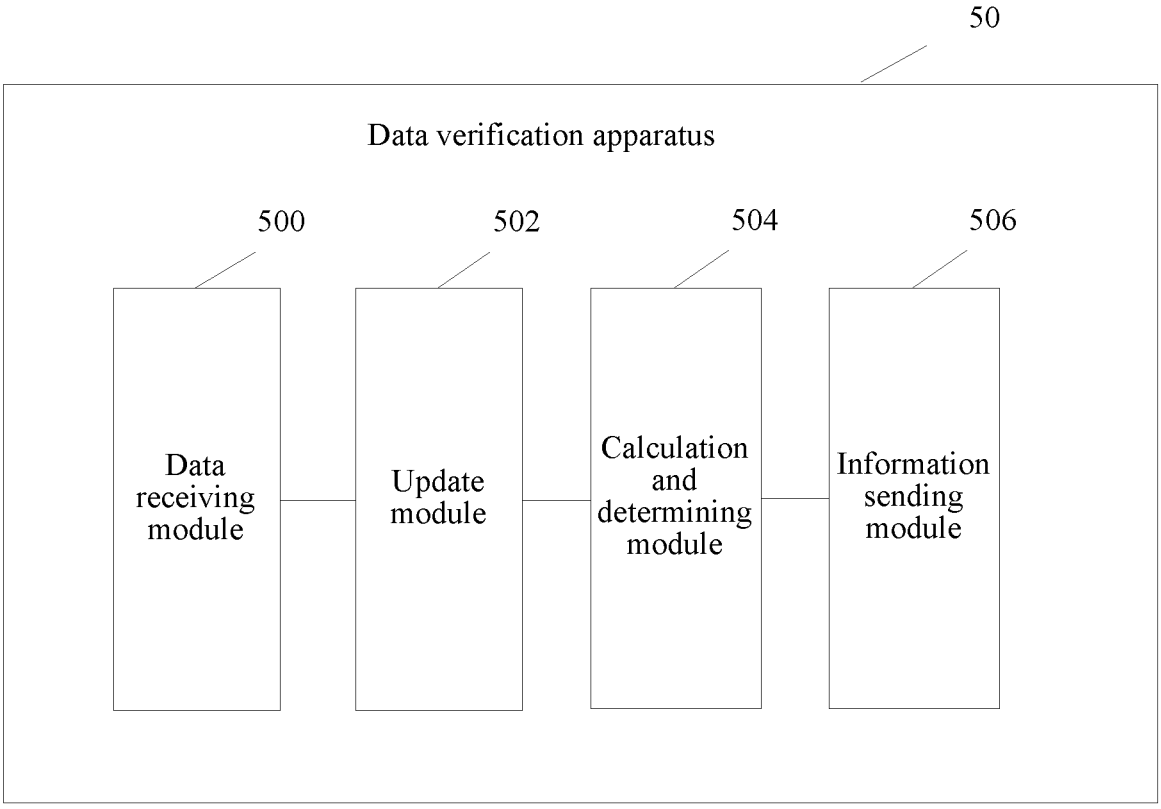
50
Data verification apparatus
500
502
504
506
Data receiving module
Update module
Calculation and determining module
Information sending module

FIG. 5B

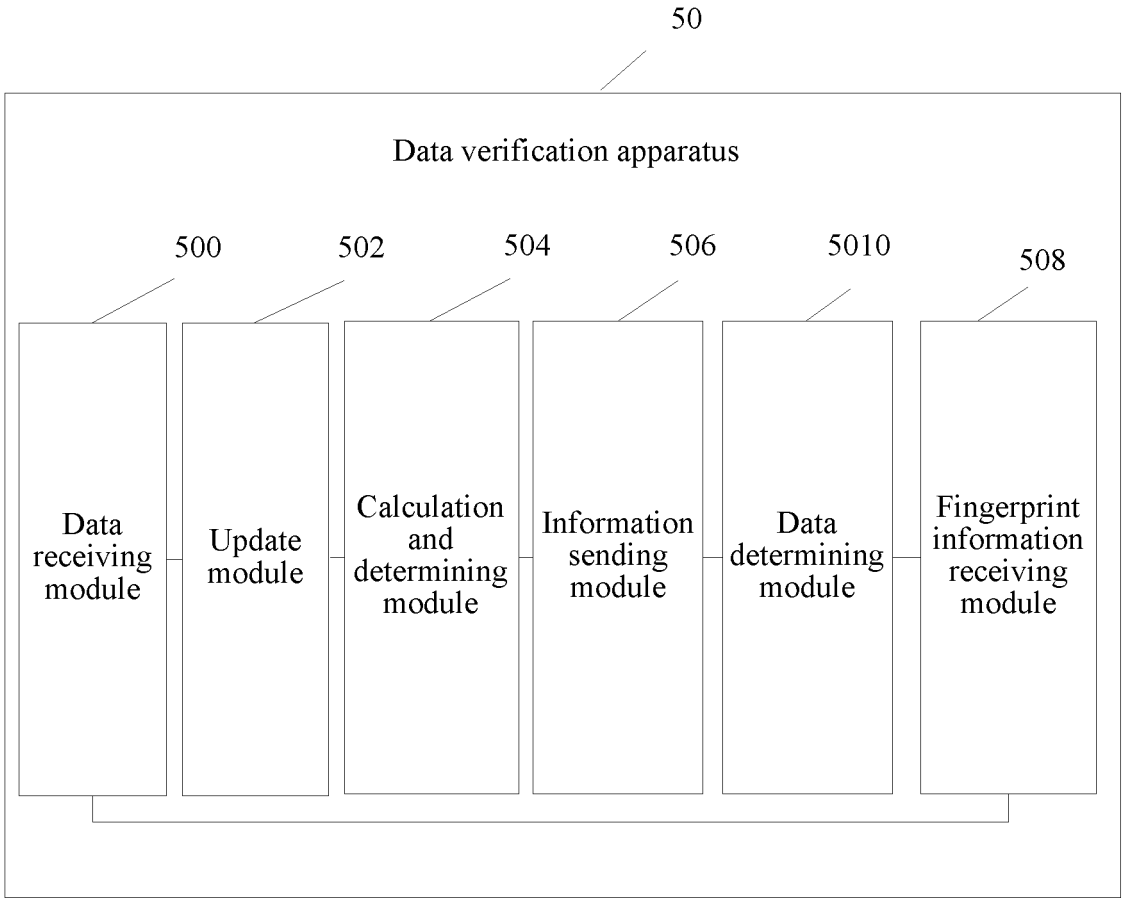
50
Data verification apparatus
500
502
504
506
5010
508
Data receiving module
Update module
Calculation and determining module
Information sending module
Data determining module
Fingerprint information receiving module

FIG. 6

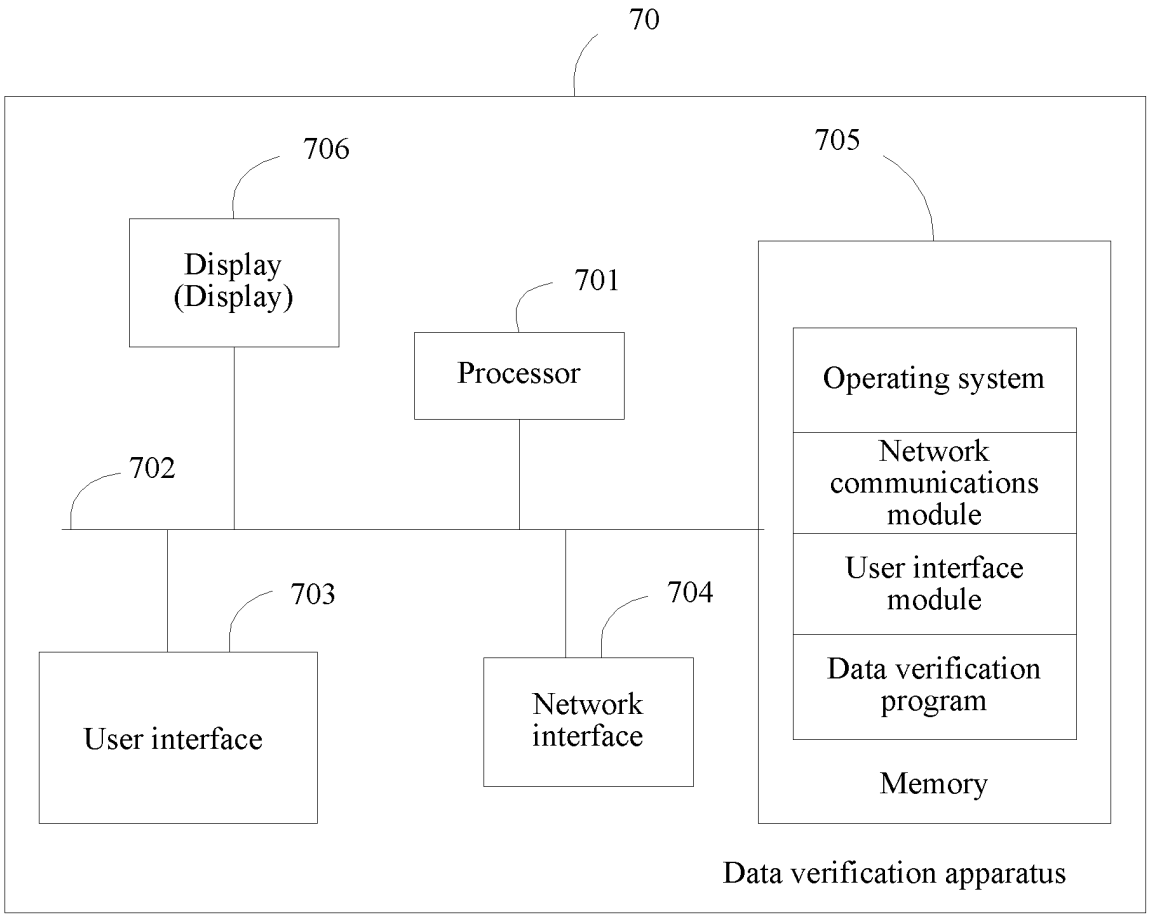
70
706
Display (Display)
705
701
Processor
Operating system
Network communications module
User interface module
Data verification program
Memory
702
703
704
User interface
Network interface
Data verification apparatus

FIG. 7

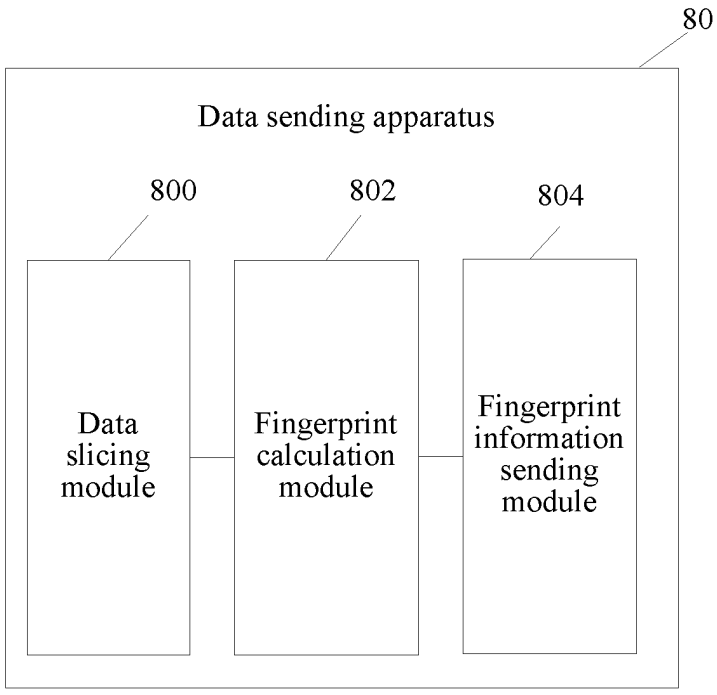
80
Data sending apparatus
800
802
804
Data slicing module
Fingerprint calculation module
Fingerprint information sending module

FIG. 8

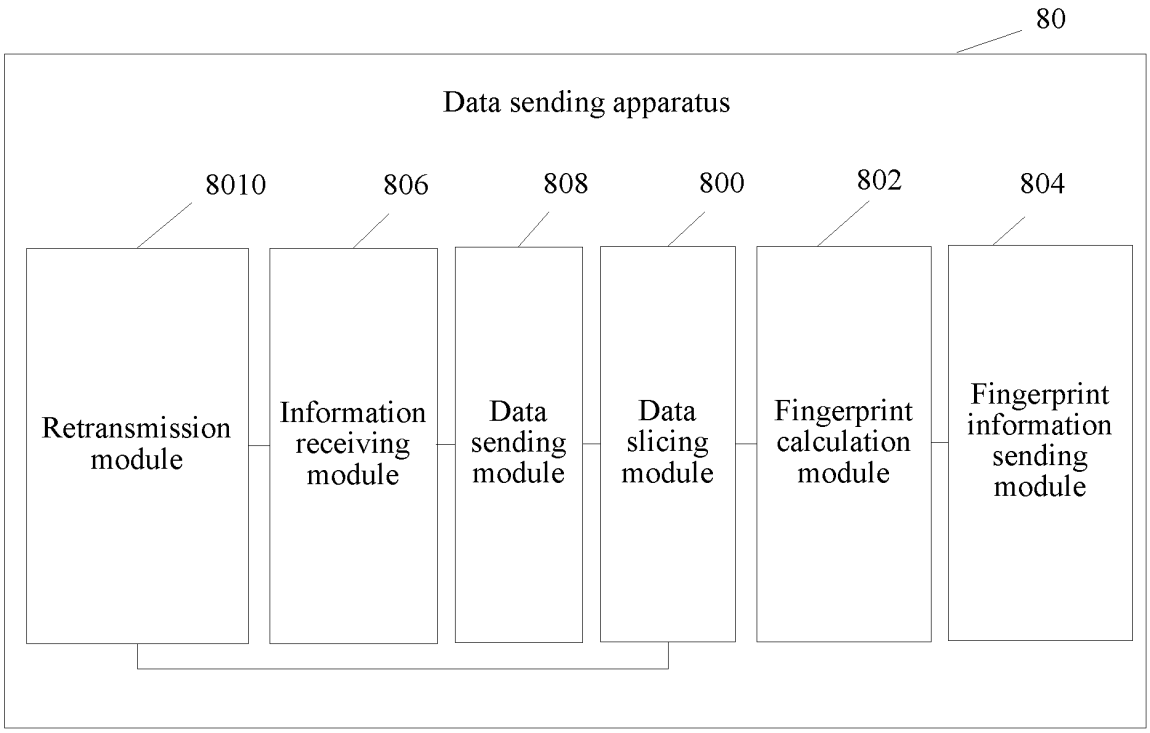
80
Data sending apparatus
8010
806
808
800
802
804
Retransmission module
Information receiving module
Data sending module
Data slicing module
Fingerprint calculation module
Fingerprint information sending module

FIG. 9

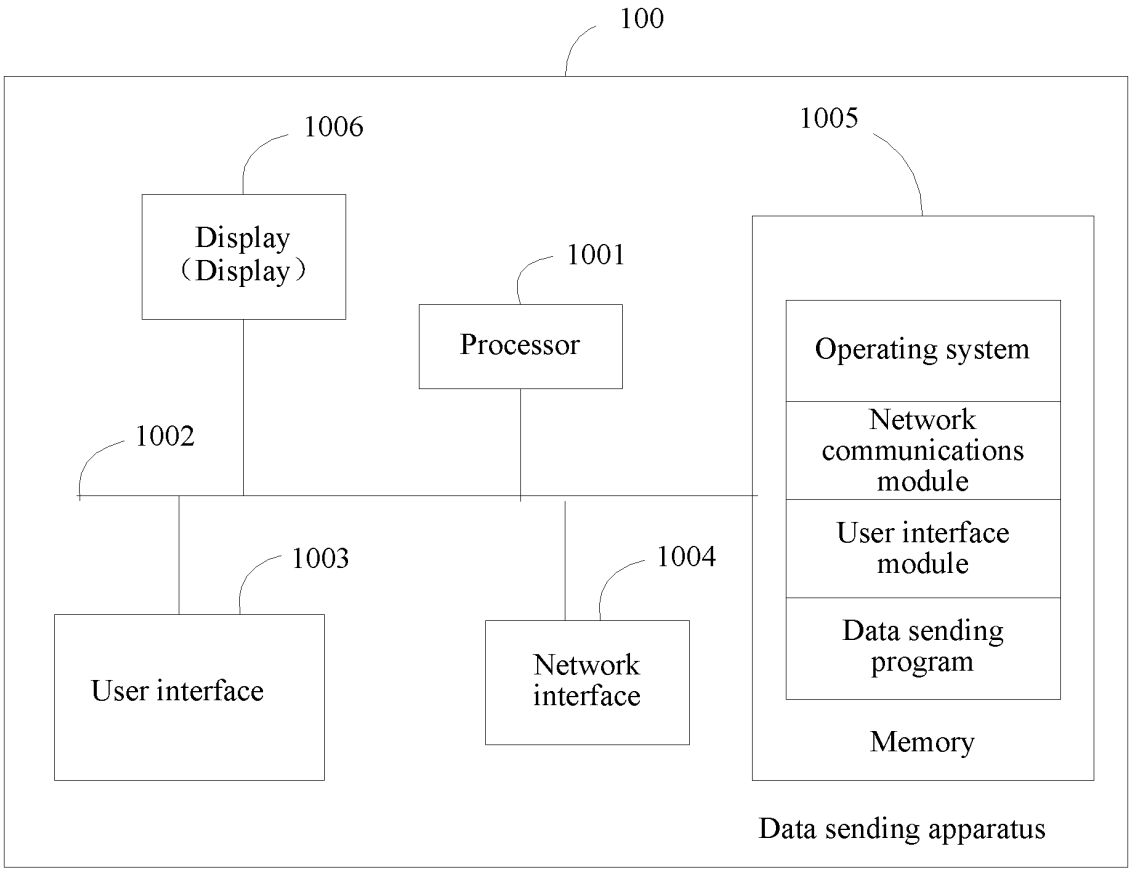
100
1006
1005
Display (Display)
1001
Processor
Operating system
Network communications module
1002
User interface module
1003
1004
Data sending program
User interface
Network interface
Memory
Data sending apparatus

FIG. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/079460

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 数据, 分片, 指纹, 顺序, 关联, 乱序, 篡改, 校验, 通过, 摘要, 消息, 更新, 对应, 云盘, 传输, 文件, 单片, 累计, data, fingerprint, hash, algorithm, abstract, value, segment, message, SHA, verify, server, client, download, cloud, storage, match, update

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102064906 A (SYNAPTIC COMPUTER SYSTEMS (SHANGHAI) CO. LTD.), 18 May 2011 (18.05.2011), description, paragraphs [0005]-[0009] and [0019]-[0044]	1-20
A	CN 101854241 A (SHANGHAI SYNACAST MEDIA TECH. CO., LTD.), 06 October 2010 (06.10.2010), entire document	1-20
A	CN 102882961 A (HUAWEI TECHNOLOGIES CO., LTD.), 16 January 2013 (16.01.2013), entire document	1-20
A	CN 101651709 A (INSTITUTE OF ACOUSTICS, CHINESE ACADEMY OF SCIENCES), 17 February 2010 (17.02.2010), entire document	1-20
A	US 8407186 B1 (SYMANTEC CORPORATION), 26 March 2013 (26.03.2013), entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 May 2018	20 June 2018

Name and mailing address of the ISA	Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	NIU, Xiaojia Telephone No. 86-010-53961761

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/079460

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102064906 A	18 May 2011	None	
CN 101854241 A	06 October 2010	None	
CN 102882961 A	16 January 2013	CN 102882961 B	17 June 2015
CN 101651709 A	17 February 2010	CN 101651709 B	05 September 2012
US 8407186 B1	26 March 2013	None	

Form PCT/ISA/210 (patent family annex) (January 2015)

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- CN 201710170866 **[0001]**